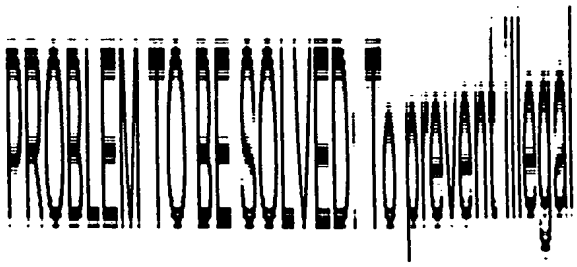
DATA TERMINAL EQUIPMENT AND COMPUTER PROGRAM

Publication number: JP10031587
Publication date: 1998-02-03
Inventor: ICHIGE KENJI
Applicant: HITACHI LTD
Classification:
- international: ***G06F21/22; G06F9/06; G06F15/00; G06F21/00;*** **G06F21/22; G06F9/06; G06F15/00; G06F21/00;** (IPC1-7): G06F9/06; G06F15/00
- European:
Application number: JP19960184406 19960715
Priority number(s): JP19960184406 19960715

Abstract of JP10031587



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－31587

(43)公開日　平成10年(1998)２月３日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ｋ
						５５０Ｅ
	15/00	３３０			15/00	３３０Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平8－184406

(22)出願日　平成８年(1996)７月15日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

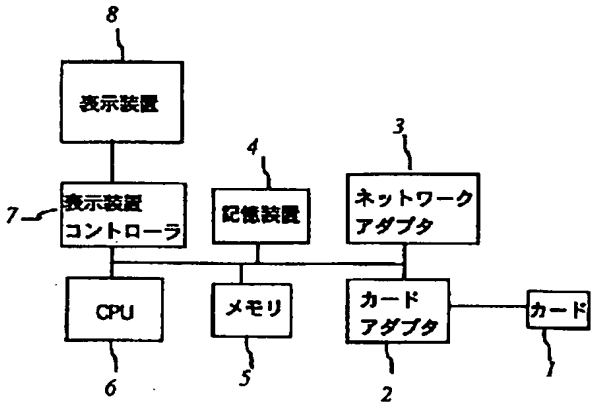
(72)発明者　市毛　健志
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　データ端末装置およびコンピュータプログラム

(57)【要約】
【目的】ネットワーク経由で配布するソフトウエアの使用権を遵守して動作するデータ端末装置を実現する。
【解決手段】使用者の公開鍵で暗号化し、ソフトウエア開発元自らがディジタル署名したデータをソフトウエア使用権のためのデータとして、移動可能な媒体に記録し、データ端末装置はソフトウエア実行時にデータを読み出して使用権を検査し、検査結果に応じてその動作を変更する。

図１

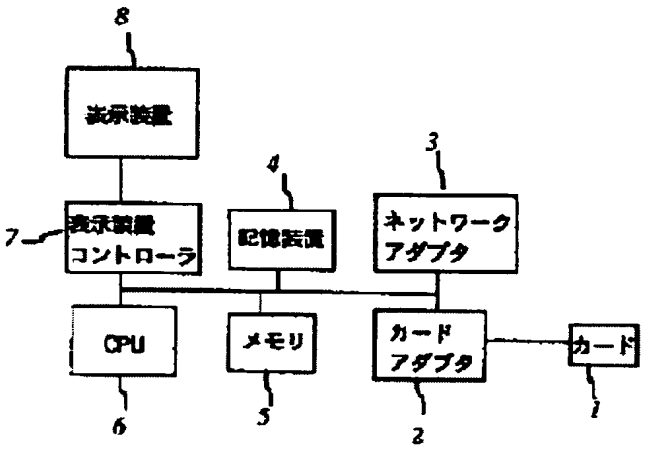


DATA TERMINAL EQUIPMENT AND COMPUTER PROGRAM

Publication number: JP10031587
Publication date: 1998-02-03
Inventor: ICHIGE KENJI
Applicant: HITACHI LTD
Classification:
- International: ***G06F21/22; G06F9/06; G06F15/00; G06F21/00;*** **G06F21/22; G06F9/06; G06F15/00; G06F21/00;** (IPC1-7): G06F9/06; G06F15/00
- European:
Application number: JP19960184406 19960715
Priority number(s): JP19960184406 19960715

Abstract of **JP10031587**

PROBLEM TO BE SOLVED: To prevent illegal use by ciphering data with the open key of a user, recording data which a software development source digitally signs in a movable medium, permitting a terminal equipment to read data and inspect use right and to change the operation in accordance with an inspected result at the time of executing software. SOLUTION: CPU 6 operates in accordance with basic software (OS) loaded on the memory 5 from a storage device 4 or a network adapter 3 and an application program and the processed result is displayed on a display device 8 through a display device controller 7. For operating the application program which the software development source develops, data which the software development source himself digitally signs is recorded in the memory 5 as data for software use right. The data terminal equipment reads data, inspects use right and changes the operation in accordance with the inspected result at the time of executing software.



1

【特許請求の範囲】

【請求項１】コンピュータプログラムを記録する記録手段と、上記記録手段より読み出した上記コンピュータプログラムを一時記憶するメモリ手段と、上記メモリ手段に記憶したコンピュータープログラムを実行する演算処理手段と、上記演算処理手段の処理結果を表示する表示装置と、外部ネットワークに接続するネットワーク接続手段と、脱着可能でかつ携帯可能な小型の脱着可能データ記憶手段と、上記脱着可能データ記憶手段を本装置に接続し、データを読み書きする脱着可能データ記憶接続手段より構成し、上記ネットワーク接続手段により上記外部ネットワークより上記コンピュータプログラムを読み込み、読み込んだ上記コンピュータプログラムは一時的に上記記憶手段に記憶するか、あるいは直接上記メモリ手段に記憶して上記演算処理手段により実行するようにし、上記脱着可能データ記憶手段には所有者の個々のコンピュータプログラムの使用権に関するデータを記憶し、上記コンピュータプログラムの実行時に上記使用権に関するデータを読み出して使用権の正当性を検査し、上記検査結果に応じて異なった動作をすることを特徴とするデータ端末装置。

【請求項２】請求項１において、上記コンピュータプログラムの使用権に関するデータは上記コンピュータプログラムの著作権所有者により公開鍵暗号化方式に基づいて作成され、著作権所有者の秘密鍵および使用権購入者の公開鍵により暗号化されたデータであるデータ端末装置。

【請求項３】請求項１において、上記コンピュータプログラムはその内部に上記脱着可能データ記憶手段に記憶された上記コンピュータプログラムの使用権に関するデータを検査するプログラムを含み、上記検査の結果に応じて処理動作を変更するようにプログラムしたコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はインターネット等の公共のネットワークにアクセスして動作するパソコン等のデータ端末装置およびその装置で実行するコンピュータプログラムに関する。

【０００２】

【従来の技術】従来のパソコン用ソフトウエアの入手方法について述べる。この入手方法は大別して二つの方法がある。第１の方法はユーザがパソコンショップへ出向き、店頭でパッケージングされたソフトウエアを購入する方法であり、第２の方法はネットワーク経由でソフトウエアをダウンロードして入手する方法である。ダウンロードとはネットワークで接続したホストコンピュータから自分のパソコン等に向かってのデータ通信によりソフトウエアをコピーすることである。

【０００３】第１の方法で購入したソフトウエアのパッケージには、１）そのソフトウエアの実行形式のプログラムが記録してある記録メディア、通常はフロッピーディスクあるいはＣＤ－ＲＯＭ、２）取扱説明書、３）ソフトウエア使用ライセンスを証明するシルアル番号（ＳＮ）、４）ソフトウエア使用ライセンス契約書等が梱包されている。ソフトウエア開発元とユーザ間のライセンス契約は記録メディア梱包を開封することにより成立するのが通常である。購入したソフトウエアを使用するためには、パソコン本体のハードディスク等の記録装置にソフトウエアの実行形式のプログラムをコピーしなければならない。この作業を一般的にインストール作業とよぶが、このインストール作業の方法はソフトウエアによって異なっている。単純に記録メディアに記録されているプログラムをコピーするだけでよいものもあれば、専用のプログラム（インストールプログラム）を実行してプログラムをコピーし、その際、シリアル番号を入力させユーザ毎に特価したプログラムをハードディスクにコピーする場合もある。あるいは、インストールの際に記録メディアにインストールを行ったことを示すデータを書き込むなどの動作をするインストールプログラムもある。シリアル番号の入力あるいは記録メディアの書換などは不正コピーの防止のためのものである。

【０００４】第２の入手方法では、記録メディアはない。取扱説明書、シリアル番号およびソフトウエア使用ライセンス契約書はデータの形で配布される。この方法の利点は簡単かつ迅速に広範囲にソフトウエアを配布できることである。第１の方法ではパッケージの箱を運送するなど流通コストがかかるが、第２の方法では構成要素はすべてのネットワーク上を伝送するだけでよい。第２の方法ではソフトウエアのアップグレードも迅速に行えるだけでなく、ソフトウエアの価格を低減することも可能である。しかし、この方法ではソフトウエアは容易に不正コピーができる欠点がある。インストールの過程でシリアル番号を入力させることでは十分な対策とはならない。

【０００５】近年のインターネットの普及によりだれでも容易にネットワークにアクセスして、ソフトウエアを入手することが可能になりつつある。ソフトウエア入手方法としては今後第２の方法が主流になると予想される。

【０００６】また、一方ではインターネットの普及に対応して、ネットワークに大きく依存して動作する新しい端末の形態が議論されている。この一例はオラクル社が１９９６年の自社の展示会で発表したネットワークコンピュータがある。これはネットワークアクセスを主たる目的とするものであり、５００ドル程度の廉価な小型の端末装置で、少ない容量の記録装置に必要なソフトウエアのみを記録し、必要に応じてネットワークにアクセスしてソフトウエアをダウンロードしながら動作するものである。ユーザの個人情報および端末の動作条件等は付

属のＩＣカードに記録し、ＩＣカードを挿入し、パスワードを入力するだけで、個人認証を行い、ユーザの好みに応じた環境を構築して動作する。

【０００７】

【発明が解決しようとする課題】しかし、二つの入手方法のどちらを選んでもソフトウエアの不正使用を完全には防止することはできない。シリアル番号による不正使用防止策では不十分なのである。シリアル番号だけなら正規のライセンス取得者の知人であれば容易に聞き出すことが可能であり、ライセンスを正規に入手せずともソフトウエアを自分のハードディスクにインストールして使用することが可能である。

【０００８】この不正使用防止策の不完全性は、ソフトウエア開発元にネットワーク経由でのソフトウエアの配布に対して消極的な態度をとらせる結果となる。

【０００９】また、従来の方法によればソフトウエアの使用はインストールを行ったパソコンのみに限定されてしまう。ある時点で複数のパソコンにソフトウエアをインストールして使用することは許可されない。他のパソコンで同一のソフトを使用するためには、以前のパソコンにインストールしたソフトを専用のソフトウエアによるかあるいは単純に削除した後に、他のパソコンにインストールしなければならない。この制限は通常ソフトウエア使用ライセンス契約書に明記されている規約事項であるが、本来購入したのはソフトウエアの使用ライセンスであるのだからライセンスを取得したものならばどのパソコンでも当のソフトウエアが使えることが望ましい。

【００１０】特にネットワーク依存型の端末では頻繁にネットワークにアクセスして、ソフトウエアをダウンロードするが、ネットワークの効率的使用のためにはソフトウエアを分散して配置してデータトラフィックの集中をさせないようにすることが望ましい。このためには適切な不正使用の検査システムが必要であるが、その動作に際してもソフトウエア開発元へのデータの集中を避けなければならない。

【００１１】シリアル番号の盗用による不正使用を摘発するための方法として、ソフトウエアの動作時にシリアル番号をネットワーク経由でソフトウエア開発元に集めて検査することが考えられるが、この方法はソフトウエア開発元にデータを集中されるものであり好ましくない。

【００１２】本発明の第１の目的は、ソフトウエアをネットワーク経由でパソコン等のネットワーク端末にダウンロードし、ソフトウエアを動作させる際に、ソフトウエアの使用ライセンス契約が正しく守られているかチェックし、不正使用を防止するシステムを提供することである。ただし、このシステムの運用がネットワーク経由でのソフトウエアの配布を促進する方向に働かねばならない。また、システムがその運用により極端にホスト側へのデータの集中を起こすものではならない。

【００１３】本発明の第２の目的はソフトウエア使用ライセンスを端末から切り離し、どの端末でも使用ライセンスを取得したソフトウエアを使用可能にすることである。

【００１４】

【課題を解決するための手段】この課題を解決するためソフトウエアライセンスをデータ化し、移動可能な媒体に記録し、ソフトウエア使用時にデータを読み出してライセンスを検査する。

【００１５】データ化のために公開鍵暗号化方式を用い、ソフトウエア開発元が使用者の公開鍵で暗号化し、かつソフトウエア開発元自らがディジタル署名したデータをソフトウエアライセンスのためのデータとする。

【００１６】ソフトウエアは実行時に移動可能な媒体からデータ読み出し、データを復号することを試みる。データが正当なものでなければ、復号化は失敗して適当な復号化データを得ることができず、ソフトウエア使用ライセンスが正しく取得されていないことを知ることができる。ソフトウエアは検査結果に基づいてソフトウエアの機能を制限あついは変更して動作する。

【００１７】

【発明の実施の形態】以下、図面を用いて本発明の実施例を説明する。

【００１８】図１は本発明の第１の実施例であり、インターネットなどのネットワークにアクセスしてソフトウエアをダウンロードし、ダウンロードしたソフトウエアを実行する装置本体の構成を示す。１は移動可能な記録媒体（カード）、２はカード１を読み書きするための記録・読みだし装置（カードアダプタ）、３はネットワークとの間でデータあるいはプログラムを送受信するネットワークアダプタ、４はハードディスクなどのソフトウエアおよびデータを記録するための記録装置、５はメモリ、６はＣＰＵ（Central Processor Unit;中央演算処理ユニット）、７は表示装置コントローラ、８は表示装置、９はキーボード・マウスなどの入力装置である。カード１、カードアダプタ２を除くと通常のパソコンと基本的には同様の構成である。

【００１９】ＣＰＵは記憶装置４あるいはネットワークアダプタ３より基本ソフト（ＯＳ）とアプリケーションプログラムをメモリ５にロードする。ＯＳおよびアプリケーションプログラムはＣＰＵに対する命令およびその他のデータにより構成されるものであり、ＣＰＵはメモリにロードしたＯＳおよびアプリケーションプログラムにしたがって動作する。ＯＳおよびアプリケーションプログラムを総称して単にプログラムと記す。記憶装置４には使用頻度の高い全部あるいは必要な部分のプログラムを記録しておき、動作時に生じるプログラムの不足分はネットワークアダプタ３を使用してネットワークよりコピーしてメモリ５にロードする。ＣＰＵの処理結果は

表示装置コントローラ７を経由して、表示装置８に送る。利用者は表示装置８を見ることにより、プログラムの動作結果を知ることができる。利用者からの指示は入力装置９よりＣＰＵに伝達される。

【００２０】カード１はカードアダプタ２に対して容易に何度でも抜き差し可能なものであり、ＣＰＵ６はカードアダプタ２に挿入したカード１のデータ内容を読み書きすることができる。このカードとしてＩＣカード、フロッピーディスクなどのメディアを使用することができる。

【００２１】図３は動作時のメモリ５の内容を示したものである。ここではユーザＢが本装置を用いてソフトウエア開発元Ａが開発したアプリケーションプログラムＰ１を動作させる場合を説明する。ユーザＢは正規にＰ１の使用ライセンスを取得しているとする。ＯＳおよびアプリケーションプログラムのプログラムサイズがメモリ５の容量に対して十分に小さいならばそれらプログラムのすべてのプログラムコードをメモリ５にロードする。そうでなければ、メモリ５にはＯＳおよびアプリケーションプログラムのプログラムコードの内の必要な部分あるいは使用頻度の高い部分のみを常駐させる。動作時に不足分が生じた場合、プログラムの不足分は記録装置４からメモリ５にロードするかあるいはネットワークアダプタ３を使用してネットワークよりコピーしてメモリ５にロードする。いずれにしろ動作時にはＯＳおよびアプリケーションプログラムの一部あるいは全部がメモリ５にロードされる。

【００２２】アプリケーションプログラムＰ１の動作の初期段階で使用ライセンスの検査を行う。このため、この段階ではＰ１のプログラム領域にはＰ１を識別するためのコードであるプログラムコードＰＩＤ、ライセンス検査プログラム、Ａ社の公開鍵ＰＫＡ、ライセンス検査プログラムがロードされ、ＯＳのプログラム領域には公開鍵暗号化プログラムと記録媒体読み書きプログラムがロードされている。

【００２３】ここで、ＰＩＤはプログラムＰ１を識別するためのコードである。プログラム名あるいはプログラム毎にユニークに決められた数字などを用いる。処理を簡単にするためには所定サイズのデータにすることが望ましい。

【００２４】ライセンス検査プログラムはＰ１の使用ライセンスをユーザが正規に取得しているかを検査するプログラムである。ユーザＢのライセンスに関するデータはカード１に記録されているので、このデータを読み出すために記録媒体読み書きプログラム３０３を呼び出して実行する。さらに、このデータを復号するために公開暗号化プログラム３０２を呼び出して実行する。

【００２５】図２はカード１に記録したデータ内容を示すものである。データ内容は所有者の公開鍵および秘密鍵、認証者の公開鍵、ライセンス管理テーブル、個々のライセンスデータより構成する。公開鍵および秘密鍵は公開暗号化方式の暗号化あるいは復号化で使用する鍵データであり、所有者の公開鍵は適当な認証者たとえば銀行あるいは公共機関などにより認証を受けたものを用いる必要がある。公開鍵の正当性を高めるため、認証者は複数であることが望ましい。ライセンス管理テーブルは複数のライセンスデータを管理するためのデータであり、図に示すように全ライセンス数、個々のライセンスデータの対応するプログラムのＰＩＤ、カード内での記憶位置、サイズより構成する。ライセンスデータはユーザの個々のソフトウエアに対するソフトウエア使用ライセンスをデータ化したものである。

【００２６】ライセンスデータはソフトウエア開発元が特定のユーザに対して該当するソフトウエアの使用ライセンスを証明するものである。具体的には、ソフトウエア開発元がユーザよりユーザの公開鍵を入手し、該当するソフトウエアが使用するデータをユーザの公開鍵により公開鍵暗号化し、暗号化したデータをソフトウエア開発元の秘密鍵により公開鍵暗号化した暗号化データあるいは同上の暗号化データをソフトウエア開発元がディジタル署名した暗号化データを用いる。ユーザの公開鍵により暗号化することにより、ユーザ以外には現実的には復元不可能なデータとなり、ユーザのみがそのライセンスデータを使用することが可能になる。ここで、現実的と限定を加えた理由は、公開鍵暗号化方式により暗号化した暗号化データを復号化の鍵の所有者以外のものが復元することは不可能とは言えないが、そのためには非現実的なほど膨大な時間あるいは費用が発生するのでできないとの意図である。以降の説明ではのような場合には現実的の限定なしに述べることとする。また、ライセンスデータ生成の最後の過程がソフトウエア開発元のディジタル署名でも暗号化でもよい理由は、どちらによってもソフトウエア開発元によって作成されたデータであることが証明されるからである。説明でユーザおよびソフトウエア開発元の秘密鍵は正しく管理され、第３者がそれを使用できない状態にあることは前提条件である。また、ユーザおよびソフトウエア開発元の公開鍵は少なくとも一つ以上の共通の認証者によって承認されていることが、相互の公開鍵の正当性の確認のために必要である。

【００２７】説明でソフトウエアが必要とするデータとは、ソフトウエア毎にその数、内容が異なってよい。そのデータはソフトウエアの動作に変化させることもあれば、その動作にはまったく無関係のデータでもよい。

【００２８】最も単純な場合の例として、データとしてソフトウエアのシリアル番号（ＳＮ）を用いることを考えることができる。これは数１により示すことができる。

【００２９】

【数１】

プログラムP1のユーザーBに対するライセンスデータL1：

$$L1 = ((SN1 * SKA) * PKB) \quad \cdots [数\ 1]$$

ただし、

*：公開鍵暗号化演算，
SN1:ユーザBに割り当てられたプログラムP1のSN，
SKA：A社の秘密鍵，
PKB：Bの公開鍵．

【００３０】

＊　＊【数２】

プログラムP1のユーザーBに対するライセンスデータL1：

$$L1 = (((SN1+X) * SKA) * PKB) \quad \cdots [数\ 2]$$

ただし、

*：公開鍵暗号化演算，
SN1:ユーザBに割り当てられたプログラムP1のSN，
X:プログラムの動作を変化させるパラメータ，
SKA：A社の秘密鍵，
PKB：Bの公開鍵．

【００３１】ここでライセンスデータはＬ１、ユーザＢの公開鍵はＰＫＢ、ソフトウエア開発元Ａの秘密鍵はＳＫＡ、プログラムＰ１のＳＮはＳＮ１、公開暗号化方式による暗号化演算は記号＊で表わす。ソフトウエア開発元Ａは数２に基づきライセンスデータＬ１を発行し、ネットワーク経由でユーザＢに送信する。ユーザＢ以外の者はライセンスデータＬ１を利用不可能なデータであり、第３者に盗聴あるいはコピーされたとしても問題は起こらない。

【００３２】前述の例より複雑な例としては、この例のＳＮに替えて、ソフトウエアの動作条件を決定するパラメータ、付加機能使用許可のためのデータ、使用期間を限定するデータなどを使用することが考えられる。ソフトウエアの動作条件を決定するパラメータの例は各国語へのローカライズのデータが考えられる。地球規模のグローバルなネットワーク上を同一のソフトウエアを配布し、動作時に各国語に応じて切り替えるだけでよい場合に対応する。付加機能使用許可のためのデータの例は、ソフトウエアの機能として一般のユーザは使用しない専門的な機能をオプションとして加える場合が考えられる。この場合、当然ながらライセンス料などの契約条件が変わることが予想される。使用期間限定のデータの例は、ソフトウエアの試用が考えられる。ソフトウエアの新規ユーザ獲得のために一定期間に限り無償で試用を許可することは有効である。この場合でも、ソフトウエア本体は正規ユーザのものと同一のものを使用することができる。この様にライセンスデータを変えることにより、同一のソフトウエアを配布しながら、個々のライセンス契約の内容に応じた動作をさせることが可能である。

【００３３】ソフトウエアの動作の過程を図５のフローチャートで説明する。ソフトウエアＰ１は記録装置あるいはネットワークアダプタよりメモリロードされた後実行される。ロード直後にソフトウエアＰ１内部のライセンス検査プログラムが実行される。このライセンス検査プログラムはカード１より対応するライセンスデータを読み出し検査する。検査結果を条件として分岐して、各結果毎（結果１、結果２、…、結果ｋ）の処理（処理１、処理２、…、処理ｋ）を行う。ここで、分岐の数ｋはプログラムに依存する数で通常２以上である。結果の中のどれかは不正なライセンスを使用した場合に対応する。

【００３４】本実施例によれば、ソフトウエアをネットワーク経由で配布する際にもライセンスを正しく管理することができ、不正使用を防止することができる。また、使用ライセンスをデータ化し、データにソフトウエア使用上の条件を内包することにより、同一のプログラムを配布しておきながらユーザ毎のライセンスの内容に応じた動作をするプログラムを提供することができる。

【００３５】

【発明の効果】本発明によればネットワーク経由で配布するソフトウエアの使用ライセンスの管理を正しく行うことができるので、ソフトウエア開発元は安心して有償のソフトウエアのネットワーク経由で出荷することができる。これによりソフトウエアのアップグレードが行われる際には世界中場所を問わず迅速なアップグレードを行うことができる。また、ネットワークによる配布による流通コストの低減、および不正コピー防止の効果により、ソフトウエア代金の低価格化に効果がある。

【図面の簡単な説明】

【図１】第１の実施例を示すブロック図。

【図２】第１の実施例における記録媒体のデータ内容を示す説明図。

【図３】第１の実施例におけるソフトウエア動作時のメモリ内容を示す説明図。

【図４】第１の実施例の装置の利用形態を示すブロック図。

【図５】第１の実施例のアプリケーションプログラムの

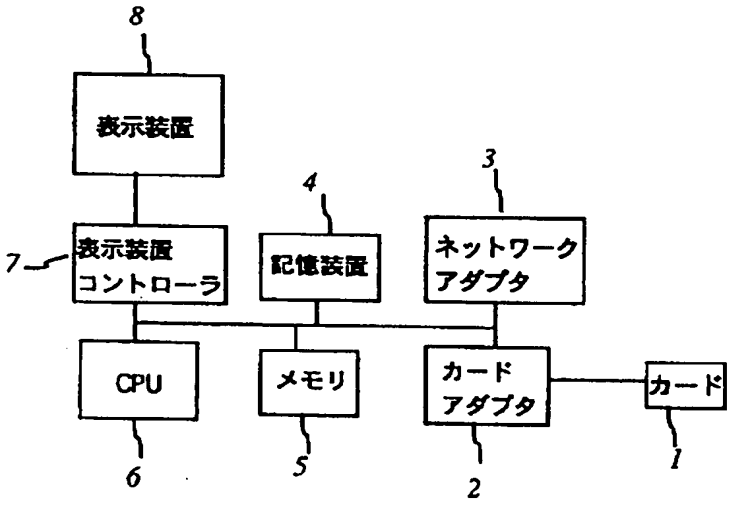
動作フローチャート。

【符号の説明】

1…移動可能な記録媒体、
2…記録媒体の記録・読み出し装置、
3…ネットワークアダプタ、
＊4…本体の記録装置、
5…メモリ、
6…ＣＰＵ、
7…表示装置コントローラ、
＊8…表示装置。

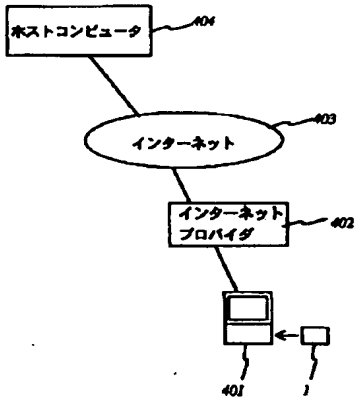
【図１】

図１



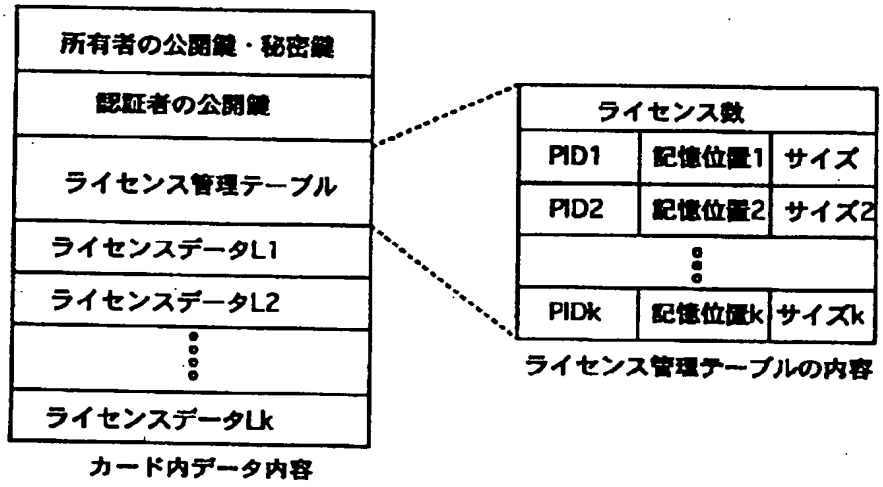
【図４】

図４



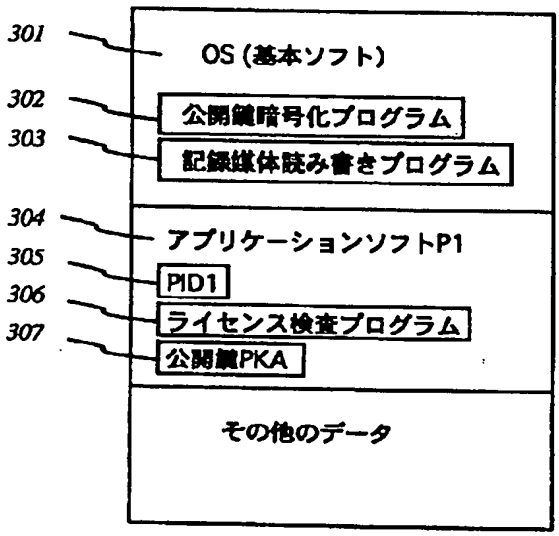
【図２】

図２



【図３】

図３



メモリの内容

【図５】

図５